

August 13, 2008

Joint Interoperability Test Command
P.O. Box 12798
Fort Huachuca, AZ 85670-2798
Attn: Mr. Jeremy Duncan

Subject: FortiGate IPv6 Letter of Compliance

To whom it may concern,

The Fortinet, Inc. FortiGate security appliance family, consisting of the product models listed below conforms to requirements for an Information Assurance Device, identified in the *DoD IPv6 Standard Profiles for IPv6 Capable Products Version 3.0, 13-Jun-2008* and the *Department of Defense Internet Protocol Version 6 Generic Test Plan, Version 3, August 2007*. All FortiGate models support the same code base and as such, all models configured with a JITC-endorsed firmware version are eligible.

The FortiGate product models differ in processing capacity and number and type of interfaces with consistent functionality including IPv6 support across all models. The FortiGate Models are: FG-50B, FWF-50B, FG-60, FG-60B, FW-60A, FW-60B, FG-100A, FG-200A, FG-224B, FG-300A, FG-310B, FG-400A, FG-500A, FG-800, FG-800F, FG-1000A, FG-1000A-LENC, FG-1000AFA2, FG-3016B, FG-3600, FG-3600LX2, FG-3600LX4, FG-3600A, FG-3810A-E4, FG-5001SX, FG-5001A, FG-5001FA2, FG-5005FA2 and FG-5005-DIST. Since these appliances are of equivalent architecture, only a representative sample will be tested to validate the product family.

These FortiGate models are compliant to the Firewall IA product class functional requirements below as indicated by the ☒, indicating that the required support is available in FortiOS v3.0. Details pertaining to the version of FortiOS providing the required IPv6 support shall be provided by Fortinet following acceptance of this Letter of Compliance.

Information Assurance (IA) Device Requirements - IPv6 Base

- ☒ RFC 1981 Path MTU Discovery for IPv6
- ☒ RFC 2460 Internet Protocol v6 (IPv6) Specification
- ☒ RFC 2461 Neighbor Discovery for IPv6
- ☒ RFC 2462 IPv6 Stateless Address Auto-configuration (Section 5.5). Global unicast addressing is not automatically configured. Only DAD and automatic link-local IPv6 address configuration is supported in the current build.
- ☒ RFC 4007 IPv6 Scoped Address Architecture
- ☒ RFC 4193 Unique Local IPv6 Unicast Addresses
- ☒ RFC 4291 IP Version 6 Addressing Architecture
- ☒ RFC 4443 Internet Control Message Protocol (ICMPv6)
- ☒ RFC 2710 Multicast Listener Discovery (MLD) for IPv6

(Required support for at least one of the below)

- ☒ RFC 2464 Transmission of IPv6 Packets over Ethernet Networks
- ☐ RFC 2467 Transmission of IPv6 Packets over FDDI Networks
- ☐ RFC 2472 IP Version 6 over PPP
- ☐ RFC 3572 IPv6 over MAPOS (Multiple Access Protocol over SONET/SDH) (JITC Recommended)

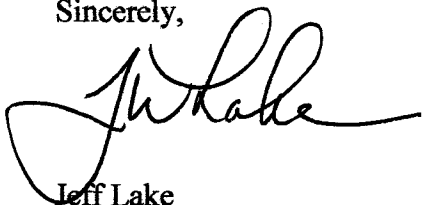
(Optional additional connection technologies)

- ☐ RFC 2491 IPv6 Over Non-Broadcast Multiple Access (NBMA) Networks
- ☐ RFC 2492 IPv6 over ATM Networks January 1999
- ☐ RFC 2497 Transmission of IPv6 Packets over ARCnet Networks
- ☐ RFC 2590 Transmission of IPv6 Packets over Frame Relay Networks Specification
- ☐ RFC 3146 Transmission of IPv6 over IEEE 1394 Networks
- ☐ RFC 4338 Transmission of IPv6, IPv4, and Address Resolution Protocol (ARP) Packets over Fibre Channel

IPSec (*FortiGates can only be certified for use with IKEv1 sessions. No IKEv2 capability currently exists*)

- ☒ RFC 2401 Security Architecture for the Internet Protocol
- ☒ RFC 2403 The Use of HMAC-MD5-96 within ESP and AH
- ☒ RFC 2405 The ESP DES-CBC Cipher Algorithm With Explicit IV
- ☒ RFC 2406 IP Encapsulating Security Payload (ESP)
- ☒ RFC 2407 The Internet IP Security Domain of Interpretation for ISAKMP
- ☒ RFC 2408 Internet Security Association and Key Management Protocol
- ☒ RFC 2409 The Internet Key Exchange (IKE)
- ☒ RFC 2410 The NULL Encryption Algorithm and its Use With IPSec
- ☒ RFC 3602 The AES-CBC Cipher Algorithm and Its Use with IPsec
- ☒ RFC 4109 Algorithms for Internet Key Exchange v1 (IKEv1)
- ☒ RFC 4835 (obsoletes RFC 4305) (ESP and AH) Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH) (*If device supports IKEv2*)
- ☐ RFC 4306 Internet Key Exchange (IKEv2) Protocol (*If device supports IKEv2*)
- ☐ RFC 4307 Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)

Sincerely,



Jeff Lake

Vice President, Federal Operations

jlake@fortinet.com

(c) 678-481-6455

(o) 678-402-8021